Oil & gas industry slow to address cyber threats

By Alec Basson

17 Sep 2020

International oil and gas companies face increased political risk because of cyber attacks and they will need to change the way they approach risk management to minimise the impact of cyber threats. This is one of the main findings of a recent study at Stellenbosch University (SU).

123rf.com

“By digitalising their systems to increase productivity and profitability, oil and gas companies are opening themselves up to even greater risk of being the target of a cyber attacks that can result in the theft or destruction of intellectual property, espionage, extortion, and massive disruption of operations,” says Kayla Mc Ewan, who obtained her master’s degree in political science at Stellenbosch University.

There is little information on the full impact of cyber attacks on the oil and gas industry despite it being targeted more than other industrial sectors. “Research conducted by multinational organisation Ernst and Young showed that the oil and gas industry face more cyber attacks (to steal intellectual property or data and financial information) and phishing attempts than other industrial sectors," she says.

Previous attacks

She says two of the most prominent cyber attacks against the oil and gas industry are those on Saudi Aramco in 2012 and Norwegian oil and gas companies in 2014.

“The Shamoon attack on Saudi Aramco showed how a cyber attack can affect a company in a major way. Not only did Saudi Aramco lost its recent drilling and production data; it was also forced to shut down its corporate operations and had to use significant financial revenue to recover. It also had to give oil away to local trucks to maintain domestic oil supply. It took the company over two months to recover.”

Management strategies

Mc Ewan adds that it is becoming increasingly important for oil and gas companies to start developing management strategies to address the risk of cyber threats.

“The industry has been slow to address the issue of cyber threats and how to manage them. Oil and gas companies, if they have been the target of a cyber attack, are normally unwilling to even say they have been a target.”

“In the case of Saudi Aramco, they had no clear risk management plans in place to effectively manage the threat or to prevent the attack from happening.”

Mc Ewan says oil and gas companies need to take a closer look at the vulnerabilities that exist throughout the industry because identifying them is a key part of developing plans to either mitigate or manage cyber threats.

“Example of these vulnerabilities include a lack of well-developed plans and programmes for monitoring and detecting of and dealing with cyber threats; the industry’s size which makes it difficult to secure all the different automated systems and Internet of Things devices; the reliance on traditional method of security and uneducated and untrained employees; and the use of different firms, suppliers and vendors with different security systems to protect their assets.”

Mitigating the risk

Mc Ewan suggests a few steps that oil and gas companies can take to mitigate the risk of cyber attacks.

She says they need to put in place technological methods of risk management such as early warning and detection systems that can act as safeguards against cyber-threats.

“They should start to deploy anti-malware reputation servers to supplement traditional, signature-based anti-virus software and also separate the business systems from operational systems. To manage the risk of cyber threats effectively, evaluation needs to be conducted continuously to detect any form of breach or inaccuracy in a facility’s system.”

Mc Ewan says oil and gas companies also need to start sharing information with one another regarding their experiences with cyber threats and steps they may have taken to manage them. They should also promoting cyber security awareness among their employees and train them accordingly.
.